## IN THE CLAIMS

Please amend the claims as follows:

1. (Canceled)

2. (Currently Amended) A storage medium containing content with protections against unauthorized copying, the storage medium comprising:

digital signature authenticating at least an identifier of the storage medium;

a revocations list for identifying at least one revoked storage medium;

content that is encrypted by using broadcast encryption, whereby:

each of a plurality of authorized playback devices has cryptographic keys sufficient for decrypting the content, and

each of a plurality of revoked playback devices does not have keys sufficient for decrypting the content;

program logic for an interpreter of a Turing complete language, the program logic ~~corresponding to~~ being a portion of the content and adapted for execution on a playback device in order to play another portion of the same content, the program logic being loaded with the content on the playback device, the program logic further configured for cryptographically authenticating the revocations list, the program logic further configured to perform a security check that interrogates a playback environment of the playback device and to verify at least one of: a playback device identity, including at least one of a player serial number, specific subscriber information, a player model, or a player software version, and a user identity, including at least one of a user name, geographical region, email address, or a web address;

a plurality of versions for each of a plurality of portions of the content, wherein:

said versions for each portion are distinguished from each other,

said versions are encrypted with different keys, such that each of said authorized playback devices is capable of deciphering at least one, but not all, of said versions for each of said portions, and

the combination of said portions decipherable by a given player being usable to identify said player, the program logic being further configured to provide a correct set of decryption keys for decrypting each of said versions decipherable by a given player, at least one decryption key of the set of decryption keys for decrypting a corresponding one of said versions decipherable by a given player; and

interface logic defining an interface usable to interact with a user and to control playback of the content by using the program logic.

3. (Previously Presented) The medium of claim 2, wherein:

said program logic is configured to perform a plurality of security checks; and

said program logic is configured to permit playback of the content provided that said plurality of security checks is successful.

4. (Previously Presented) The medium of claim 3 wherein said program logic is configured to invoke at least one cryptographic operation supported by at least one of said authorized playback devices.

5. (Previously Presented) The medium of claim 3 wherein said program logic is configured to perform at least one operation necessary for decryption of the content by at least one said authorized playback device.

6. (Previously Presented) The medium of claim 2 wherein a subset of said authorized playback devices encompass a plurality of models, each model having a model-specific vulnerability, and the medium further comprising program logic which, when executed by a device of each said vulnerable model, is configured to:

mitigate said vulnerability affecting said vulnerable playback device; and

perform at least one operation necessary for said vulnerable playback device to decrypt said content.

7. (Previously Presented) The medium of claim 6 wherein said program logic includes executable code for a Turing-complete virtual machine.

8. (Previously Presented) The medium of claim 6 wherein said operation necessary to decrypt includes updating a cryptographic key contained in said playback device.

9. (Previously Presented) The medium of claim 6 wherein said program logic for mitigating includes native executable code configured to detect whether security of a vulnerable device has been compromised.

10. (Previously Presented) The medium of claim 6 wherein said program logic for mitigating includes native executable code configured to correct a vulnerability in a vulnerable device.

11. (Previously Presented) The medium of claim 6 wherein said program logic for mitigating includes a firmware upgrade for correcting at least one vulnerability.

12. (Currently Amended) A device for securely playing content, the content including a plurality of regions each having multiple versions thereof, the device comprising:

a media reader for use in reading data from a storage medium;

a nonvolatile memory containing:

a set of cryptographic player keys for use with a broadcast encryption system, and identifiers of revoked media;

a bulk decryption module for decrypting encrypted content from the storage medium;

a Turing-complete interpreter for executing program logic, the program logic ~~corresponding to~~ being a portion of the content and configured to:

load with the content from the media reader, the program logic being adapted for execution on the device in order to play another portion of the same content on the device;

cryptographically authenticate identifiers of revoked media;

interrogate a playback environment of the device and to verify at least one of: a device identity, including at least one of a player serial number, specific subscriber information, a player model, or a player software version, and a user identity, including at least one of a user name, geographical region, email address, or a web address;

verify whether digital signatures contained on the storage medium authenticate the storage medium;

verify whether the storage medium is identified as revoked in said nonvolatile memory;

select a version of each of the plurality of regions, thereby generating a set of selected versions;

provide a correct set of decryption keys for decrypting each of said selected versions, at least one decryption key of the set of decryption keys for decrypting a corresponding one of said versions; and

decrypt said selected version, whereby a combination of said versions selected in the course of playing content from the storage medium uniquely identifies said device; and

at least one codec for decoding content.

13. (Previously Presented) The device of claim 12, wherein said interpreter is configured to obtain said program logic from said media reader for loading on the device.

14. (Previously Presented) The device of claim 12 further comprising means for reducing during a rendering process the output quality of said audiovisual content in dependence upon whether a security requirement specified by the storage medium for high-quality output is met.

15. (Canceled)

16. (Currently Amended) A method for playing encrypted content from a storage medium, the method comprising:

verifying a digital signature for authenticating said medium;

retrieving at least one player key from a nonvolatile memory;

using said at least one player key with a broadcast encryption system;

using a result of said broadcast encryption system to decrypt at least a portion of the content;

reading program logic for a Turing-complete interpreted language from the medium, the program logic ~~corresponding to~~ being a portion of the content, the program logic being adapted for execution on a media player device in order to play another portion of the same content on the media player device;

using an interpreter to execute said program logic, wherein said interpreter performs operations specified in said program logic including:

cryptographically authenticating identifiers of revoked media;

interrogating a playback environment of the device and to verify at least one of: a device identity, including at least one of a player serial number, specific subscriber information, a player model, or a player software version, and a user identity, including at least one of a user name, geographical region, email address, or a web address;

verifying whether digital signatures contained on the medium authenticate the medium;

verifying whether the medium is identified as revoked in said nonvolatile memory;

selecting a variant from a plurality of variants for each of a plurality of portions of the content, wherein:

said media player device for decrypting said selected variant; and

said media player device lacks at least one cryptographic key required to decrypt at least one non-selected variant for each portion;

providing a correct set of decryption keys for decrypting each selected variant, at least one decryption key of the set of decryption keys for decrypting a corresponding one of said selected variants; and

decrypting each selected variant by using the provided correct set of decryption keys.

17. (Previously Presented) The method of claim 16 wherein said interpreter performs operations specified in said program logic to respond to selections from a user, said user selections include button presses on a remote control.

18. (Previously Presented) The method of claim 16 wherein said program logic directs said player to perform an AES block cipher operation via said interpreter.

19. (Previously Presented) The method of claim 16 further comprising accessing a media revocations list to determine whether said medium has been revoked.

20. (Previously Presented) The device of claim 12 wherein:

said set of cryptographic player keys is unique to the device; and

said program logic is configured to select a unique set of versions by using said unique set of cryptographic player keys.

21. (Previously Presented) The medium of claim 3, wherein the program logic that is configured to perform a plurality of security checks generates a security check result, the security check result for embedding into content rendered by a playback device on which the security checking is performed.

22. (Currently Amended) The medium of claim 2, wherein the program logic is adapted to perform at least one security check, the at least one security check to verify ~~at least one of:~~

~~a playback device identity, including at least one of a player serial number, specific subscriber information, a player model, or a player software version, or~~

a result of cryptographic processing adapted to fail a verification operation if executed on at least one of an unauthorized or revoked or compromised playback device.

23. (Canceled)

24. (Previously Presented) The device of claim 12 wherein the program logic being configured to forego decryption of the selected version if the program logic identifies said media as revoked.

25. (Currently Amended) The method of claim 16 wherein said program logic performs at least one security check of a player device seeking to play said content, the at least one security check adapted to verify ~~at least one of:~~

~~a player identity, including at least one of a player serial number, specific subscriber information, a player model, or a player software version, or~~

a result of cryptographic processing adapted to fail a verification operation if executed on at least one of an unauthorized or revoked or compromised player, and to inhibit at least one of full quality playback or reduced quality playback if at least one security check fails.